(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
1 avril 2004 (01.04.2004)

PCT

(10) Numéro de publication internationale
WO 2004/027688 A2

(51) Classification internationale des brevets[7] : G06K 1/00

(21) Numéro de la demande internationale :
PCT/FR2003/050055

(22) Date de dépôt international :
19 septembre 2003 (19.09.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/11657 19 septembre 2002 (19.09.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **STMICROELECTRONICS SA** [FR/FR]; 29, Boulevard Romain Rolland, F-92120 MONTROUGE (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **DEVEAUD, Vincent** [FR/FR]; 2, Impasse du Bonelli, F-13710 Fuveau (FR). **LIARDET, Pierre-Yvan** [FR/FR]; 56, rue du Pralou, Lotissement L'Audiguier, F-13790 Peynier (FR).

(74) Mandataire : **CABINET MICHEL DE BEAUMONT, Michel**; 1, rue Champollion, F-38000 Grenoble (FR).

(81) États désignés *(national)* : JP, US.

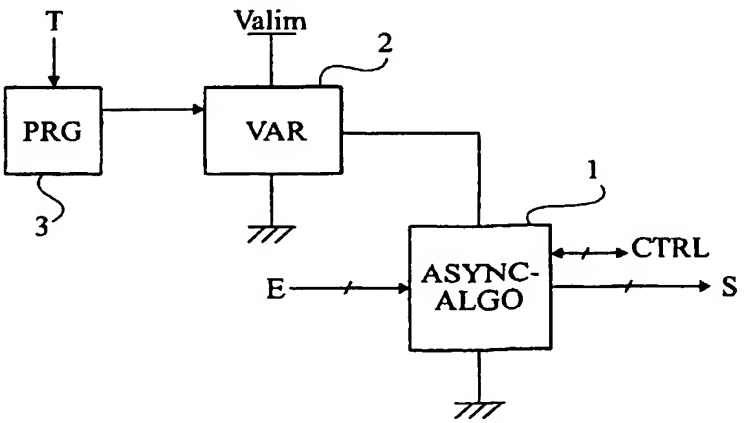
(84) États désignés *(régional)* : brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

Publiée :
— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(54) Title: POWER SUPPLY FOR AN ASYNCHRONOUS DATA TREATMENT CIRCUIT

(54) Titre : ALIMENTATION D'UN CIRCUIT DE TRAITEMENT ASYNCHRONE DE DONNEES



(57) Abstract: The invention relates to a method and feed circuit for an asynchronous calculation element (1) of an integrated circuit, wherein the instantaneous power supply of the calculation element is randomly varied .

(57) Abrégé : L'invention concerne un procédé et circuit d'alimentation d'un élément de calcul asynchrone (1) d'un circuit intégré, dans lequel on fait varier aléatoirement l'énergie instantanée d'alimentation de l'élément de calcul.

WO 2004/027688 A2

ALIMENTATION D'UN CIRCUIT DE TRAITEMENT ASYNCHRONE DE DONNÉES

La présente invention concerne les circuits intégrés ou éléments de circuit intégré exécutant de façon asynchrone des traitements de données numériques. L'invention concerne plus particulièrement les circuits manipulant des données que l'on souhaite protéger, par exemple, des données confidentielles ou des clés d'authentification.

Un type répandu d'attaque de données d'un circuit intégré exécutant des algorithmes sécurisés consiste à analyser la consommation du circuit intégré ou de la partie de celui-ci exécutant l'algorithme manipulant des données secrètes. De telles attaques par analyse de consommation sont connues sous des abréviations SPA (Single Power Analysis) ou DPA (Differential Power Analysis) et consistent à analyser la consommation d'un circuit intégré en fonction des données qu'il traite afin de découvrir des données censées être secrètes.

Dans un circuit fonctionnant de façon asynchrone, le circuit fournit les données de sortie en même temps qu'une information comme quoi ces données sont disponibles, une fois qu'il a terminé le traitement. Une attaque par analyse de la consommation d'un circuit asynchrone consiste à observer les pics d'énergie qui correspondent en fait à des données (aux instants où ces données sont traitées). Il est alors possible,

pour un pirate, de découvrir l'algorithme ou les données secrètes manipulées.

Pour essayer de masquer les traitements de données, une solution connue consiste à ajouter des circuits de traitement supplémentaires, inutiles pour le processus sécurisé proprement dit, mais qui consomment de l'énergie lorsqu'ils manipulent les données. Les données manipulées par le processus asynchrone à protéger sont alors en quelque sorte masquées par l'énergie prélevée par les circuits de traitement additionnels.

Outre le fait que l'efficacité d'une telle solution est en quelque sorte proportionnelle au nombre de circuits de traitement supplémentaires prévus, donc à l'encombrement supplémentaire dans le circuit intégré, elle ne fait qu'augmenter le nombre de combinaisons de données possibles que le pirate doit évaluer.

En fait, si la consommation additionnelle dépend des données traitées, ces données restent vulnérables. Si la consommation additionnelle est indépendante des données traitées, elle représente en quelque sorte un bruit qui peut être éliminé par des méthodes statistiques.

En outre, ajouter des traitements augmente la consommation.

La présente invention vise à proposer une autre solution pour protéger l'exécution d'un processus algorithmique asynchrone contre des attaques par analyse de la consommation du circuit intégré ou de la partie de circuit exécutant ce processus.

La présente invention vise notamment à proposer une solution dont l'efficacité ne soit pas liée à l'encombrement supplémentaire dans le circuit intégré.

L'invention vise également à proposer une solution qui ne se traduise pas simplement par une augmentation des combinaisons possibles devant être examinées par le pirate.

Pour atteindre ces objets et d'autres, la présente invention prévoit un procédé d'alimentation d'un élément de calcul asynchrone d'un circuit intégré, consistant à faire

varier aléatoirement l'énergie instantanée d'alimentation de l'élément de calcul.

Selon un mode de mise en oeuvre de la présente invention, on répartit aléatoirement, dans une fenêtre temporelle prédéterminée, l'énergie instantanée fournie à l'élément de calcul, l'énergie totale dans la fenêtre étant prédéterminée.

Selon un mode de mise en oeuvre de la présente invention, l'énergie totale fournie à l'élément de calcul dans la fenêtre temporelle est déterminée en fonction de la consommation maximale possible de l'élément de calcul.

La présente invention prévoit également un circuit d'alimentation d'au moins un élément de traitement asynchrone d'un circuit intégré, comportant un élément d'alimentation variable commandé de façon aléatoire ou pseudo-aléatoire.

Selon un mode de réalisation de la présente invention, ledit élément d'alimentation variable fait varier la tension d'alimentation de l'élément de traitement asynchrone.

Selon un mode de réalisation de la présente invention, l'élément d'alimentation variable est commandé par un générateur pseudo-aléatoire.

Ces objets, caractéristiques et avantages, ainsi que d'autres de la présente invention seront exposés en détail dans la description suivante de modes de mise en oeuvre et de réalisation particuliers faite à titre non limitatif en relation avec les figures jointes parmi lesquelles :

la figure 1 représente, de façon très schématique et sous forme de blocs, un mode de réalisation d'un circuit d'alimentation d'un élément de calcul asynchrone selon la présente invention ; et

la figure 2 illustre, par un chronogramme, un mode de mise en oeuvre du procédé d'alimentation selon l'invention.

Pour des raisons de clarté, seuls les étapes de procédé et éléments de circuit qui sont nécessaires à la compréhension de l'invention ont été représentés aux figures et seront décrits par la suite. En particulier, l'algorithme mis en oeuvre

par l'élément de calcul à protéger n'a pas été détaillé et ne fait pas l'objet de l'invention, celle-ci s'appliquant quel que soit le processus asynchrone mis en oeuvre. De plus, l'élément de calcul asynchrone est bien sûr le plus souvent associé à d'autres éléments de circuit avec lequel il est intégré. On ne fera référence ci-après qu'à l'élément de calcul asynchrone et à son alimentation, l'invention n'agissant pas sur le reste du circuit qui dépend de l'application.

Une caractéristique de la présente invention est de faire varier aléatoirement l'énergie fournie à l'élément de traitement asynchrone des données à protéger.

La présente invention tire profit du fait que, dans un élément de traitement asynchrone, un défaut d'énergie par rapport à l'énergie nécessaire à la manipulation d'une donnée ne se traduit pas par une erreur de fonctionnement mais simplement par un retard dans le traitement des données. En effet, un élément de traitement asynchrone attend en quelque sorte d'avoir l'énergie nécessaire au traitement pour poursuivre son calcul.

Dans les circuits classiques, la source d'énergie est suffisante pour fournir à l'élément de traitement toute l'énergie qu'il requiert à chaque instant. Selon l'invention, on impose l'énergie fournie à l'élément de traitement.

Par exemple, on utilise un générateur pseudo-aléatoire tenant compte de la durée souhaitée pour le calcul afin de répartir la quantité d'énergie nécessaire à ce calcul dans une fenêtre temporelle.

En effet, la seule contre-partie de la mise en oeuvre de l'invention est un allongement de la durée d'exécution. Cette durée d'exécution peut cependant être maintenue dans une fenêtre prédéterminée grâce à une génération pseudo-aléatoire.

Si l'application le permet, notamment si elle n'impose pas de contraintes temporelles, on peut utiliser un générateur aléatoire qui présente l'avantage de dissocier non seulement l'alimentation mais également la durée par rapport aux données traitées. La durée de traitement est ainsi rendue aléatoire.

La figure 1 représente, de façon partielle très schématique et sous forme de blocs, un mode de réalisation d'un circuit d'alimentation d'un élément 1 d'exécution asynchrone d'un algorithme de traitement de données (ASYNC-ALGO). De façon classique, l'élément de calcul asynchrone peut être schématisé comme un circuit recevant des données d'entrée E, fournissant des données de sortie S et échangeant des signaux de commande (CTRL) avec le reste du circuit intégré (par exemple, avec un microprocesseur non représenté). Parmi les signaux de commande figure notamment le signal par lequel l'élément 1 indique au reste du circuit intégré que les données de sortie S sont disponibles.

Selon l'invention, le circuit 1 est alimenté au moyen d'un circuit 2 (VAR). Le circuit 2 fournit une énergie variable au circuit 1 et est alimenté par une tension Valim, par exemple, la tension d'alimentation du circuit intégré. Au sens de l'invention, la variation d'énergie peut être effectuée en tension ou en courant, en respectant si besoin les contraintes d'alimentation minimales (par exemple, en niveau de tension) afin de ne pas perdre les données en cours de traitement par le circuit asynchrone 1.

Selon le mode de réalisation représenté en figure 1, le circuit 2 de variation de l'alimentation est commandé par un générateur 3 pseudo-aléatoire (PRG) afin de distribuer l'énergie de façon aléatoire tout en respectant une fenêtre temporelle T prédéterminée correspondant à la durée souhaitée pour l'exécution du calcul. Le générateur 3 reçoit la consigne T, par exemple, de l'unité centrale du circuit intégré fixant la fenêtre temporelle.

Dans le cas où un même circuit intégré contient plusieurs éléments de traitement asynchrone distincts, ceux-ci peuvent être alimentés séparément les uns des autres ou de façon commune au moyen d'un même générateur variable 2.

La figure 2 illustre le fonctionnement du circuit de la figure 1 par un organigramme représentant l'énergie (PW)

fournie au circuit 1 dans une fenêtre temporelle T d'exécution du calcul.

En figure 2, on a représenté par un pointillé p, ce que pourrait être l'énergie absorbée par le circuit 1 dans un cas classique, si celui-ci était directement alimenté par la tension Valim sans recours au générateur variable 2 propre à l'invention. Dans ce cas, l'élément 1 prélève autant d'énergie qu'il en a besoin instantanément. C'est ce qui permet à un pirate éventuel d'analyser les pics de consommation et de relier ces pics aux données (bits 0 ou 1) traitées. Selon l'invention, la même quantité d'énergie nécessaire à l'exécution de l'ensemble du calcul est répartie temporellement dans la fenêtre T de façon aléatoire.

Comme cela a été indiqué ci-dessus, la seule conséquence est un allongement de la durée du calcul par rapport au cas classique. Toutefois, cet allongement peut être si besoin limité à une fenêtre temporelle prédéterminée du générateur pseudo-aléatoire.

Un avantage de la présente invention est qu'elle permet de masquer les données manipulées par un élément asynchrone de façon particulièrement efficace et, notamment, sans que cela se traduise par une augmentation des combinaisons à examiner par le pirate éventuel. En effet, aucun traitement (calcul) supplémentaire des données n'est prévu par l'invention. Par conséquent, l'efficacité du système n'est pas liée à l'accroissement de l'encombrement des circuits de traitement.

Un autre avantage de l'invention est qu'elle ne nécessite aucune modification de l'élément de traitement asynchrone proprement dit. On se contente d'intervenir sur son alimentation. Cet avantage conduit notamment à ce que l'invention puisse être mise en oeuvre dans n'importe quel processus de traitement asynchrone existant sans engendrer de modifications de la partie calcul du circuit intégré existant.

Un autre avantage de la présente invention est qu'elle n'engendre pas de consommation énergétique supplémentaire pour

l'exécution du calcul lui-même, contrairement aux solutions requérant des circuits de traitement additionnels.

La mise en oeuvre pratique de l'invention à partir des indications fonctionnelles données ci-dessus est à la portée de l'homme du métier. En particulier, la réalisation d'un générateur variable alimentant un élément de calcul asynchrone ne nécessite que des composants classiques et est à la portée de l'homme du métier.

Bien entendu, la présente invention est susceptible de diverses variantes et modifications qui apparaîtront à l'homme de l'art. En particulier, la détermination du niveau d'énergie minimal éventuel qu'il faut fournir à un élément de traitement asynchrone pour préserver les données qu'il est en train de traiter dépend de l'application et l'homme du métier sera à même de fixer les seuils adaptés. Par exemple, on pourra fixer un seuil minimal de tension d'alimentation et faire varier aléatoirement la tension d'alimentation du circuit de traitement dans une plage prédéterminée. Enfin, la réalisation d'un générateur d'une consigne aléatoire ou pseudo-aléatoire fait appel à des moyens classiques qui sont à la portée du l'homme du métier.

REVENDICATIONS

1. Procédé d'alimentation d'un élément de calcul asynchrone (1) d'un circuit intégré, caractérisé en ce qu'il consiste à répartir aléatoirement, dans une fenêtre temporelle prédéterminée (P), l'énergie instantanée d'alimentation de l'élément de calcul, l'énergie totale dans la fenêtre étant prédéterminée.

2. Procédé selon la revendication 1, caractérisé en ce que l'énergie totale fournie à l'élément de calcul dans la fenêtre temporelle est déterminée en fonction de la consommation maximale possible de l'élément de calcul.

3. Circuit d'alimentation d'au moins un élément de traitement asynchrone (1) d'un circuit intégré, caractérisé en ce qu'il comporte un élément d'alimentation variable (2) de l'élément de traitement asynchrone, ledit élément d'alimentation répartissant de façon aléatoire et dans une fenêtre temporelle prédéterminée, l'énergie instantanée fournie à l'élément de calcul, l'énergie totale dans la fenêtre étant prédéterminée.

4. Circuit selon la revendication 3, caractérisé en ce que l'élément d'alimentation variable (2) est commandé par un générateur pseudo-aléatoire (3).

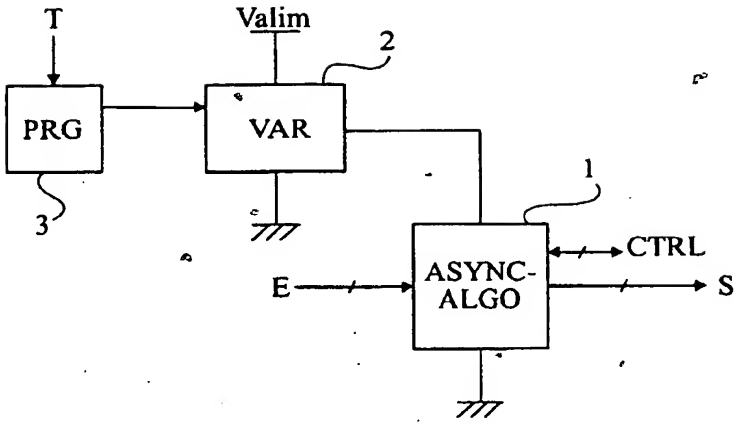


Fig 1

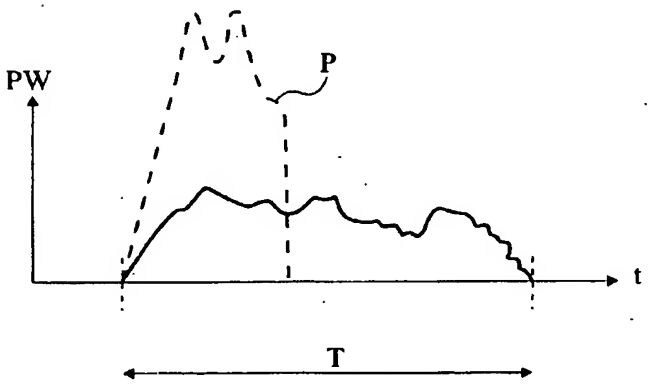


Fig 2